Újgenerációs adat- és hálózatbiztonsági módszerek

Doktori értekezés tézisei

Vörös Péter

Témavezető: Dr. Kiss Attila

Eötvös Loránd Tudományegyetem
Informatikai Kar
Információs Rendszerek Tanszék

Informatikai Doktori Iskola
Iskolavezető: Prof. Csuhaj-Varjú Erzsébet
Doktori Program: Információs Rendszerek
Programvezető: Prof. Benczúr András

Budapest, 2019

Bevezetés

Az okostelefonok és a különböző online szolgáltatások terjedésének köszönhetően manapság az emberek hihetetlen mennyiségű adatot generálnak. A Cisco új Visual Networking Index (VNI) jelentése szerint 2022-ben az internetes adatforgalom nagyobb lesz, mint az internet elindítása óta eltelt 32 év alatt összesen. Az egyre okosabb eszközöknek köszönhetően egyre szenzitívebb információkat osztunk meg magunkról akár szándékosan akár tudtunkon kívül. Ez a hatalmas adatmennyiség, és a kezelésükért felelős szolgáltatások egészen új adattárolási és adatbiztonsági kihívásokkal szembesítik a szakértőket.

A technológia jelen fejlettségi szintje messze túl komplex ahhoz, hogy az átlag emberek pontosan tisztában legyen a rendszerek működésének részleteivel. Ez egyrészről teljesen érthető, hiszen nem lehet mindenki informatikai szakember, ugyanakkor mégis sajnálatosnak tartom, hogy az átlagos internethasználók többségének elképzelése sincs róla, hogy mi számít biztonságosnak, vagy, hogy milyen kockázatai vannak egy adathalász oldalon megadott bankkártyaadatnak. Szerencsére ezzel együtt az látható, hogy a felhasználók egy másik csoportja is kezdi kinőni magát, akiknél komolyan megjelenik az igény arra, hogy biztonságban tudják az adataikat.

A dolgozatban bemutatom az aktuális szolgáltatások elleni leggyakoribb támadási típusokat, a támadások felépítését, és különböző védelmi módszereket dolgozok ki a mind a szolgáltatók mind a felhasználók számára. Azonosítom a különböző védelmi pontokat, és azokat az általam tervezett eszközöket/szolgáltatásokat is bemutatom amik ezeken a pontokon vethetőek be annak érdekében, hogy a szenzitív adatok kompromittálhatatlanságát megőrizzük.

Tézisek

1 Biztonsági megoldások szolgáltatóknak generációs csomagtovábbítás a hálózati biztonságban

A hosszú távú rendszerek kialakításának kulcsa, hogy könnyen bővíthetők és a holnap igényei szerint konfigurálhatók legyenek. Most egy olyan korszak felé haladunk, ahol minden eszköz okos és minden mindennel össze van kapcsolva. Éppen ezért szükségünk van arra, hogy hálózati rendszereinket egyszerűen bővíthetővé tudjuk tenni. A korábbi ver-

tikálisan integrált hálózatok nem tették lehetővé a meglévő protokollok megváltoztatását anélkül, hogy elképesztő mennyiségű extra munkát kellene elvégezni.

Ezeket a korábbi megközelítésű, a fix protokollokra kialakított rugalmatlan hálózati eszközöket fokozatosan váltotta le az SDN [15][14]. (Software Defined Networking) szemlélet. Ezt a más megközelítésű magasabb absztrakciós szintről programozható hálózatot az operátorok sokkal könnyebben változtathatják az igényekhez igazítva.

A sok különböző magas szintű nyelv közül a P4 [12] (Programming Protocol-independent Packet Processors) a fix protokollmezők limitációnak a feloldását helyezte elsődleges céljának azzal, hogy a csomagok leírása absztrakt módon protokollfüggetlenül megtehető benne. Az OpenFlow-hoz képest ez sokkal nagyobb szabadságot jelent a hálózat programozásában

1. Tézis: A P4 nyelvvel lehetséges magas absztrakciós szintű logikával hatékony protokoll- és hardverfüggetlen tűzfal implementálása.

Kapcsolódó publikációk: [3] [4] [6] [7] [9]

A dolgozat 1.1. fejezetében bemutattam az új generációs csomagtovábbítás által kínált lehetőségeket, illetve a P4-et mint magas absztrakciós szintű csomagtovábbítási logikát leíró nyelv. Ismertettem a T4P4S nevű P4 fordítónk működését, megmutattam, hogy a fordított switch program képes a hardverre optimalizált binárisokéval közel megegyező sebességű csomagtovábbításra. Ezután pedig adtam egy lehetséges módszert a P4, második generációs - állapottal rendelkező csomagszűrő tűzfalként való felhasználására.

DDoS támadások modellezése és IDS-ek

Hatékony védelmi stratégiák létrehozása az informatikai biztonságban elengedhetetlen, viszont ez gyakran nagyon nagy kihívást jelent. A 2014-es Cyberthreat Védelmi Jelentés szerint [18], amely több mint 750 biztonsági döntéshozót és szakembert vont be, a szervezetek több mint 60%-a ellen követtek el betöréses támadásokat 2013-ban.

A big data elemzés a biztonságban, lehetőséget ad a digitális adatok tömeges összegyűjtésére és elemzésére a támadások előrejelzése és megelőzése érdekében. Mivel azonban a szükséges adatok hatékony, teljes és megbízható módon történő összegyűjtése problémás feladat, az iparág számára hasznos lehet egy olyan eszköz, amely lehetővé teszi a biztonsági védelmi algoritmusok hatékonyságának mérését és javítását. Ebből a célból bemutatunk egy olyan platformot, amely képes szimulált internetes forga-

lom előállítására számos paraméterezési lehetőséggel, a támadásmentes és rosszindulatú hálózati forgalmi minták kombinációjából. A munkához az ns3 esemény-vezérelt hálózati szimulátort használjuk. Annak érdekében, hogy a kapott adatállomány megfeleljen a behatolásérzékelő rendszer benchmarking céljainak, vizsgáljuk meg a normál és támadó forgalmi minták statisztikai jellemzőit.

2. Tézis: Készíthető olyan IDS-ek validálására használható adatgenerátor, amivel adott szerver karakterisztikáknak megfelelő HTTP forgalom generálható.

Kapcsolódó publikációk: [2]

Az 1.2. fejezetben megmutattam, hogyan épülnek fel az elosztott szolgáltatásmegtagadással járó (DDoS) támadások. Eljárást dolgoztam ki annak érdekében, hogy az elárasztás típusú DDoS támadások modellezhetőek legyenek. A HTTP forgalomra érvényes tulajdonságokat megtartva olyan gazdagon paraméterezhető forgalomgenerátort készítettem, amivel a behatolásdetektáló (IDS) rendszerek tesztelhetőek.

2 Felhasználói adatvédelem publikus felhőkben

Szerver oldali védelem

Szolgáltatóként az egyik legfontosabb feladatnak kell tekinteni a felhasználók és azok adatainak biztonságban tartását, de a gyakorlat azt mutatja, hogy a weboldalak gyakran a védtelenek a legismertebb támadási típusokkal szemben is. A weboldalak jelentős része csak a bejelentkezési oldalon használ titkosított csatornát (HTTPS-t), amely egyrészt érthető, mert a teljes kommunikáció titkosítása túlzottan erőforrásigényes lehet, ugyanakkor a titkosítás hiányából fakadó a biztonsági rés nagy támadási felületet eredményezhet. Különösen akkor, ha a szolgáltató a session cookie-kat sem védi eléggé.

A HTTP egy állapotmentes protokoll, amely azt jelenti, hogy a felhasználók csak egy specifikusan kiadott felhasználói azonosítóból ismerhetők fel. Ezt a kliens egy cookie-ként tárolja. Azt a konkrét cookie-t -amely a felhasználói munkamenetet azonosítja- session cookie-nak nevezzük. A session-hijacking olyan támadási típus, ahol a támadó valamilyen módon megszerzi az áldozatnak a session cookie-ját. Majd ennek a cookie-nak

a segítségével a támadó megtévesztheti a szervert és hamisan az áldozatként azonosítható. Így mindenhez jogosultságot szerez, amihez eredetileg az áldozatnak hozzáférése volt.

3. Tézis: One Time Token alapú szerver oldali biztonsági keretrendszerrel jelentősen javítható a Session hijacking támadás elleni védelem.

Kapcsolódó publikációk: [5]

A dolgozat 2.1. fejezetében bemutattam a session hijacking és data breach támadásokat, ami kettő a 12 legmagasabb prioritású fenyegetések közül. Elemeztem a HTTP és HTTPS forgalmak veszélyeit, a munkamenet eltérítéses támadások néhány lehetséges módját, illetve felvázoltam egy one time token alapú hitelesítő működési modelljét. Megmutattam, hogy a TooKie nevű eszközöm az egyszer használható tokenekkel, hogyan tudja HTTP-n keresztül is biztonságossá tenni a munkameneteinket.

Kliensoldali és proxy alapú védelem

A felhasználók által termelt adat mennyisége napról napra növekszik. A szociális hálózatok, az IoT, a szenzorok stb. mind mind felelősek ezért a növekedésért. Sajnos rengeteg felhasználó nincs tisztában a saját adatainak fontosságával. A vállalatok jelentős összeget fordítanak adatok biztosítására, üzleti szektoruk, méretük és költségvetésüknek megfelelően, mivel meg kell védeniük ipari titkait, szellemi tulajdonukat stb. Úgy gondoljuk, hogy ugyanez vonatkozik az otthoni felhasználókra is, mivel a támadások jelentős hányada ezeket az adatokat célozza meg, hiszen nemcsak a vállalatok adatai képviselik az üzleti értéket, hanem a felhasználóké is. A Forrester Consulting, a tanulmányukban a legértékesebb ügyfél-azonosítási adatokat mutatta be marketing célokra [17]. 2018-ig ellopták az emberek adatainak milliárdjait, amint azt a CSO jelentése is mutatja [16], ez is rámutat arra, hogy adataikat biztosítani kell.

Az adattárolási trendeket tekintve megállapítottuk, hogy a legtöbb otthoni felhasználó mellett néhány vállalat harmadik féltől származó tárhelyet is használ, amelyek többsége felhőalapú. Az EU 2014-es statisztikái azt mutatják, hogy a régióban átlagosan 21 százalék a felhőtárolót használja a fájlok tárolására, míg a maximális érték 42 százalék [13]. A végfelhasználók számára a Dropbox, a OneDrive és a Google Drive a legnépszerűbb választások közé tartozik, ami érthető, mivel ezek a szolgáltatások magas rendelkezésre állása és egyetemes hozzáférhetősége, valamint hogy ezek a szolgáltatók ingyenes tárolási kapacitást kínálnak mind mind kívánatos jellemzők. Adatbiztonsági intézkedései ellenére

a felhasználó nem tudja igazán befolyásolni, hogyan tárolják és védik az adatait. Emiatt előfordulhat, hogy a szolgáltató hozzáférhet a felhasználó adataihoz. A harmadik felek eléréséhez használt csatorna is veszélybe kerülhet, ha a szolgáltató nem garantálja biztonságát. Ha ez megtörténik, az adatok hozzáférhetővé válhatnak a man-in-the-middle támadók számára.

Számos javaslat és megoldás áll rendelkezésre adataink biztonságos megőrzésére, de sajnos eddig semmi sem vált széles körben elfogadottnak. Úgy vélem, hogy ennek fő oka a megoldásnak szánt szoftverek használatának bonyolultsága és a felhasználók tudásának valamint tudatosságának hiánya a biztonsági területen. Ezekben a tanulmányban célom volt, hogy egy könnyen használható ügyféloldali módszert adjak ahhoz, hogy a felhasználói adatok hozzáférhetetlenek legyenek mások számára a nyilvános felhőkben.

4. Tézis: Az OpenWebCrypt böngészőbe épülő alkalmazás és a CrypStorePI security middleware alkalmasak az egyes felhasználói adatok, vagy az egész privát hálózat védelmére Data Breach támadásokkal szemben.

Kapcsolódó publikációk: [1] [8] [10]

A dolgozat 2. fejezetének második felében módszereket mutattam be az egyszerű felhasználók, és a nagyobb céges hálózatok extra védelmi rétegének implementálására. Az OpenWebCrypt kliens oldali böngésző bővítménnyel elérhető egyes szolgáltatásokban tárolt felhasználói adatok elkódolása. CrypStorePI-vel pedig egy teljes hálózat válik védhetővé egy proxy elven működő security middleware használatával.

Szteganográfia és kriptográfia a felhasználói adatokhoz naptárakban

A felhasználók naponta nagy mennyiségű személyes adatot generálnak az online szolgáltatások, például a szociális hálózatok, a keresőmotorok stb. használatával, anélkül, hogy feltennék maguknak a kérdést, hogy mennyire értékesek az adataim a szolgáltatók számára? Mivel a személyes adatok gyűjtése és osztályozása a célzott hirdetések elengedhetetlen eleme, a válasz: nagyon értékes. Mivel a marketingesek egyre nagyobb mértékben támaszkodnak az ügyféladatokra, azok értéke jelentősen nőtt az elmúlt évtizedben. Egyre több adatot tárolnak különböző felhőkben, és ezzel elveszik a felhasználó lehetősége azok biztonságban tartására, mivel a szolgáltatók többsége nem kínál semmilyen lehetőséget

a megbízható titkosítás beállítására. Ebben a tanulmányban arra törekszünk, hogy bemutassuk a személyes adatoknak a kíváncsi személyektől való elrejtésének egy lehetséges módját.

Két rétegű biztonsági technikát hoztunk létre a felhasználók személyes adatainak védelmére. Az első réteg a szteganográfia, amely egy fájl, üzenet, kép vagy videó más, üzenet, kép vagy videó fájlban való elrejtését valósítja meg. Használhatjuk ezt arra is, hogy megtévesszük a támadót azzal, hogy egyáltalán észrevegye azt, hogy az általuk hozzáférhető információ hamis vagy valódi. Katzenbeisser et. al [11] szteganográfiát részletesen a bemutatja. Szótáralapú algoritmust használunk, amely kódolt szövegadatokat hoz létre, ami úgy néz ki, mint egy normál felhasználói bemenet, amely az ellenfél becsapására és az érzékeny adatok elrejtésére szolgál. A második réteg egy egyszerű, személyes jelszó alapú titkosítás, amely egyszerű stream cipher-rel kódolja az adatokat.

5. Tézis: Készíthető olyan eljárás amivel naptárbejegyzéseket más értelmesnek tűnő bejegyzésre titkosítunk el ezáltal elrejtve a rejtjelezés tényét.

Kapcsolódó publikációk: [10]

A 2. fejezet végén gyakorlati példában mutattam be, hogy hogyan használható a szteganográfia bizonyos szolgáltatások esetén arra, hogy elfedjük az adatok titkosításának tényét a támadók elől.

Szerző publikációi

[1] Vörös Péter and Kiss Attila. “Felhő architektúrák biztonsága”. In: *INFODIDACT 2014: Informatika Szakmódszertani Konferencia. Konferencia.* Vol. 16. 9789631206272. Webdidaktika Alapítvány. 2014, 9–p.

[2] Dániel Csubák et al. “Big data testbed for network attack detection”. In: *Acta Polytechnica Hungarica* 13.2 (2016), pp. 47–57.

[3] Sándor Laki et al. “High speed packet forwarding compiled from protocol independent data plane specifications”. In: *Proceedings of the 2016 ACM SIGCOMM Conference*. ACM. 2016, pp. 629–630.

[4] Péter Vörös and Attila Kiss. “Security middleware programming using P4”. In: *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, Cham. 2016, pp. 277–287.

[5] Péter Vörös and Attila Kiss. “TooKie: A New Way to Secure Sessions”. In: *Recent Developments in Intelligent Information and Database Systems*. Springer, 2016, pp. 195–207.

[6] Tamás Lévai et al. “The Price for Programmability in the Software Data Plane: The Vendor Perspective”. In: *IEEE Journal on Selected Areas in Communications* 36.12 (2018), pp. 2621–2630.

[7] Fabricio Rodriguez et al. “BB-gen: A packet crafter for P4 target evaluation”. In: *Proceedings of the ACM SIGCOMM 2018 Conference on Posters and Demos*. ACM. 2018, pp. 111–113.

[8] Péter Vörös and Attila Kiss. “OpenWebCrypt—Securing Our Data in Public Cloud”. In: *Modern Approaches for Intelligent Information and Database Systems*. Springer, 2018, pp. 479–489.

[9] Péter Vörös et al. “T4P4S: A Target-independent Compiler for Protocol-independent Packet Processors”. In: *International Conference on High Performance Switching and Routing* (2018).

[10] Péter Vörös, Péter Hudoba, and Attila Kiss. “Steganography and Cryptography for User Data in Calendars”. In: *Asian Conference on Intelligent Information and Database Systems*. Springer. 2019, pp. 241–252.

További publikációk

[11] Stefan Katzenbeisser and Fabien Petitcolas. *Information hiding techniques for steganography and digital watermarking*. Artech house, 2000.

[12] Pat Bosshart et al. “P4: Programming protocol-independent packet processors”. In: *ACM SIGCOMM Computer Communication Review* 44.3 (2014), pp. 87–95.

[13] *EUStats: Use of Internet Cloud storages*. 2014. URL: `http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet\_and\_cloud\_services\_-\_statistics\_on\_the\_use\_by\_individuals` (visited on 02/17/2018).

[14] Nuno P Lopes et al. "Checking beliefs in dynamic networks". In: *Proceedings of the 12th USENIX Symposium on Networked Systems Design and Implementation, NSDI*. Vol. 15. 2015.

[15] opennetworking.org. *SDN Definition*. 2015. URL: https://www.opennetworking.org/sdn-resources/sdn-definition (visited on 10/10/2015).

[16] *CSO: Biggest data breaches of the 21st century*. 2017. URL: https://images.idgesg.net/images/article/2017/10/biggest-data-breaches-by-year-and-accounts-compromised-1-100738435-large.jpg (visited on 02/16/2018).

[17] *Forrester Consulting: Most valuable customer data*. 2017. URL: https://www.marketingcharts.com/wp-content/uploads/2017/06/LiveIntentForrester-Most-Valuable-B2C-Customer-Identification-Data-June2017.png (visited on 02/10/2018).

[18] *CyberEdge - 2014 Cyberthreat Defence Report for North America and Europe, a CyberEdge report sponsored by ForeScout Technologies, Inc., 2014*.